关于主体机系统中的微机病毒

辽化计算中心 陈蓉生

一、前言

随着微机仿真作为主体机的终端及网关，中小型计算机系统中使用的微机就越来越多了，我公司的IBM4341系统中，现有微机6台MS-DOS病毒问题也成为我们头痛的问题。

二、病毒感染情况

我们利用公安部门提供的软件清除了BLOODY病毒，1575病毒，但是后来在查无病毒但死机情况下，开始研究原因，先后发现了主BOOT区病毒、BOOT区病毒、文件病毒等共7种，大部分不知其名，从未遇到过病毒发作所表现的屏幕及破坏磁盘现象，只遇到有病毒时，死机。

可作微机的MEMOREX汉字终端，虽然可以运行MS-DOS程序，但由于我们只作终端使用，因此从未感染过病毒。

点对点通信微机曾感染过病毒，但执行只作通信机用后，再没有感染过病毒。

公共使用的仿真终端，3+网工作站微机则反复不断的感染病毒，而且是反复感染一、两种病毒，刚消毒不几天，又发现被同一种病毒感染，而且3+网工作站上按装有某厂家的防病毒卡。

DIR-II病毒在我们机器内存在时间最长，当有了消毒软件后才彻底消除。

有一种BOOT病毒，至今无消毒软件可用，只能用复盖来消毒，因此这个病毒现在仍然反复出现。

三、病毒来源探讨

病毒程序非一般人能编得出来，我们至今没有顺利的读通过一个病毒程序，编病毒程序需要十分了解MS-DOS操作系统，具有相当的编程技巧。因此可以断定：软件公司的一些有一定水平的不逞之徒为其主要生产源。

病毒能够进入我们机房的微机内，通过以下途径：

1.按装软件时，我们发现卖方提供的网络软件盘上就有病毒。

2.运行游戏程序，我们认为玩游戏是最大的病毒来源，，游戏程序在人们之间反复拷贝，带入病毒的机会非常多。而且一些人热衷于玩游戏，更增加了感染的机会。

3.由于操作人员不了解病毒的传染过程，而误将病毒带入微机，作为数据传送的软盘，其中并无MS-DOS系统，EXE,COM等可执行软件，即使在有病毒机上感染了BOOT病毒也不会传染。但是如果将该软盘关机时忘在机器内，而且在A驱动器上，当再开机时，虽然自举失败，但是此时微机则已感染了病毒。

四、对策

1.加强管理。配备懂技术的专人定期检查、消毒，只会用查病毒软件消病毒是不行的。反复地出现病毒，都是由于软盘检查不彻底，而从新将病毒带入微机。

严禁在计算机上玩游戏，必须在制度上、行政检查上加以保证。

2.加强对操作病毒的了解。作为计算机系统工程师，计算机软件工程师应对现有的操作系统的病毒有所了解，只会在一、二种现成工具软件上作开发的，不能算是个合格的工程师。

3.使用合法软件，这不仅对避免病毒有效，而且对遇到问题，搞二次开发也是有用的。但是，这对习惯于不考虑软件投资的单位的领导来说，确实是个大大的难题。而且对整个计算机界，也还有许多工作要去做。